Digital Egypt Pioneers Initiative

Final Project

Implementing a Secure Multi-Branch Office Network

Team Members

Moahmed Nasser Mohamed Elshamy

Mohamed Moomen Abd El Hamid

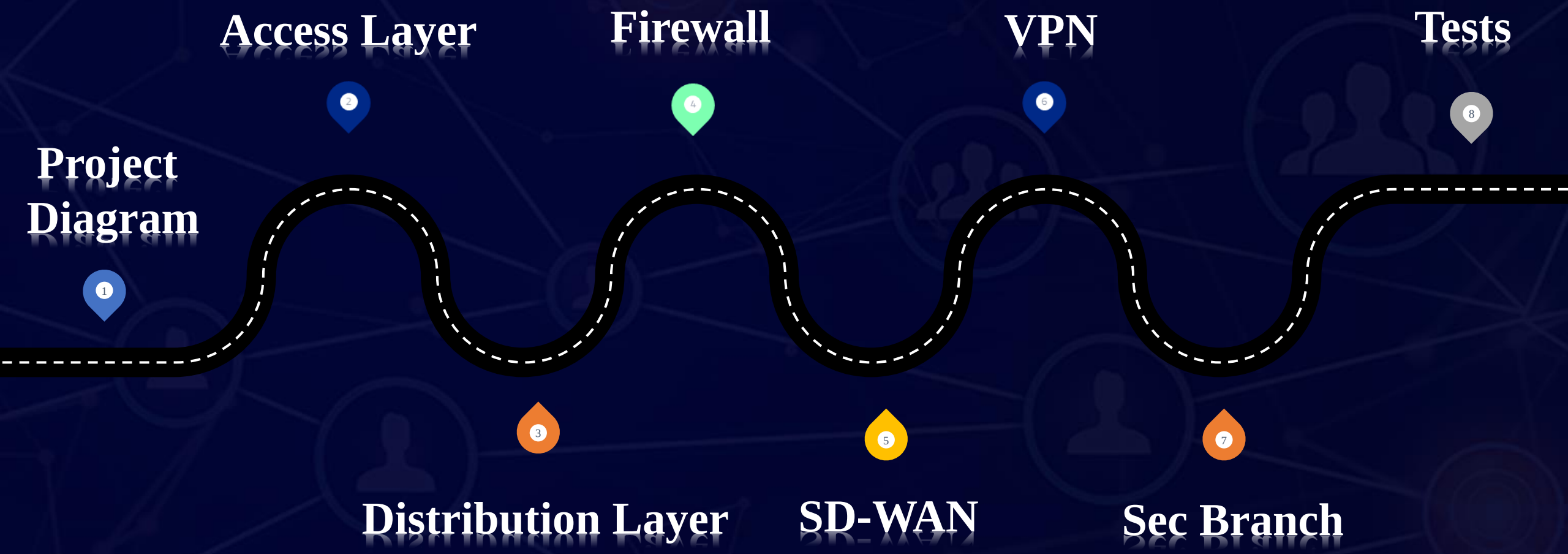
Hazem Ahmed Saad Abdel Aziz

Imad Abdel Hamid Ali Attia

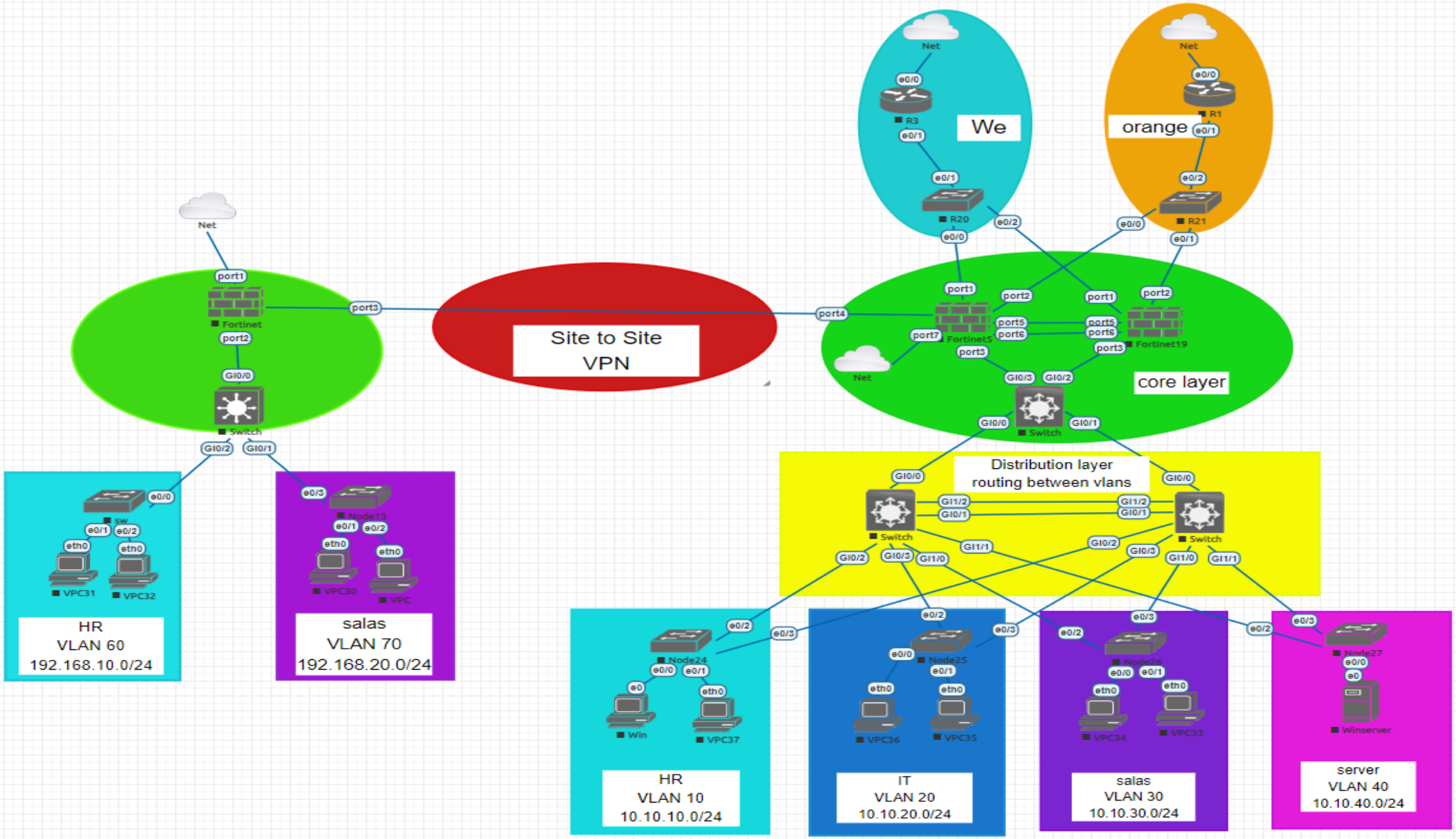
Moustafa Hossam Hassien

Mohamed Hosny Mohamed

Content


Project Diagram
1
Access Layer
2
Distribution Layer
3
Firewall
4
SD-WAN
5
VPN
6
Sec Branch
7
Tests
8

1 Project Diagram


Net
port1
Fortinet
port2
port3
Gi0/0
Switch
Gi0/2
Gi0/1
Site to Site
VPN
port4
Net
R3
e0/0
e0/1
We
R20
e0/2
Net
R1
orange
R21
port1
port2
port5
port6
port7
Fortinet5
port3
Fortinet19
Gi0/3
core layer
Distribution layer
routing between vlans
Gi1/2
Gi1/1
Gi1/0
sw
VPC31
VPC32
HR
VLAN 60
192.168.10.0/24
Node13
VPC30
VPC
salas
VLAN 70
192.168.20.0/24
Node24
Win
VPC37
HR
VLAN 10
10.10.10.0/24
Node25
VPC36
VPC35
IT
VLAN 20
10.10.20.0/24
Node26
VPC34
VPC33
salas
VLAN 30
10.10.30.0/24
Node27
Winserver
server
VLAN 40
10.10.40.0/24

2 Access layer

➢ Access Layer

- ❑ The access layer grants end devices access to the network. In the WAN environment, it may provide teleworkers or remote sites access to the corporate network across WAN connections.
- ❑ Generally incorporates Layer 2 switches and access points providing connectivity and serves a number of functions including:
  - ➢ Layer 2 switching
  - ➢ High availability
  - ➢ Port security
  - ➢ Address Resolution Protocol (ARP) inspection
  - ➢ Rapid PVST
  - ➢ Basic setting (SSH - ACL for ssh)

configuration

All access switch

```
En
Conf  t
Hostname  access –sw
Username  cisco  password  cisco
Enable  password  cisco
Banner  motd  & no unathorised access &
No  ip  domin-lookup
Service  password-encryption
Line  console  0
Password  cisco
Login  local
Exec-timeout  00
Logging  synchronous
Exit
Ip domin-name  cisco.com
Crypto  key  generate  rsa  general  key  modalus  1024
Ip ssh  version  2
Line  vty  0  15
Login  local
Transport  input  ssh
Exit
Access-list  1  permit  192.168.30.0  0.0.0.255
Access-list  1  deny  any
Line  vty  0  15
Access-class  1  in
Exit
```

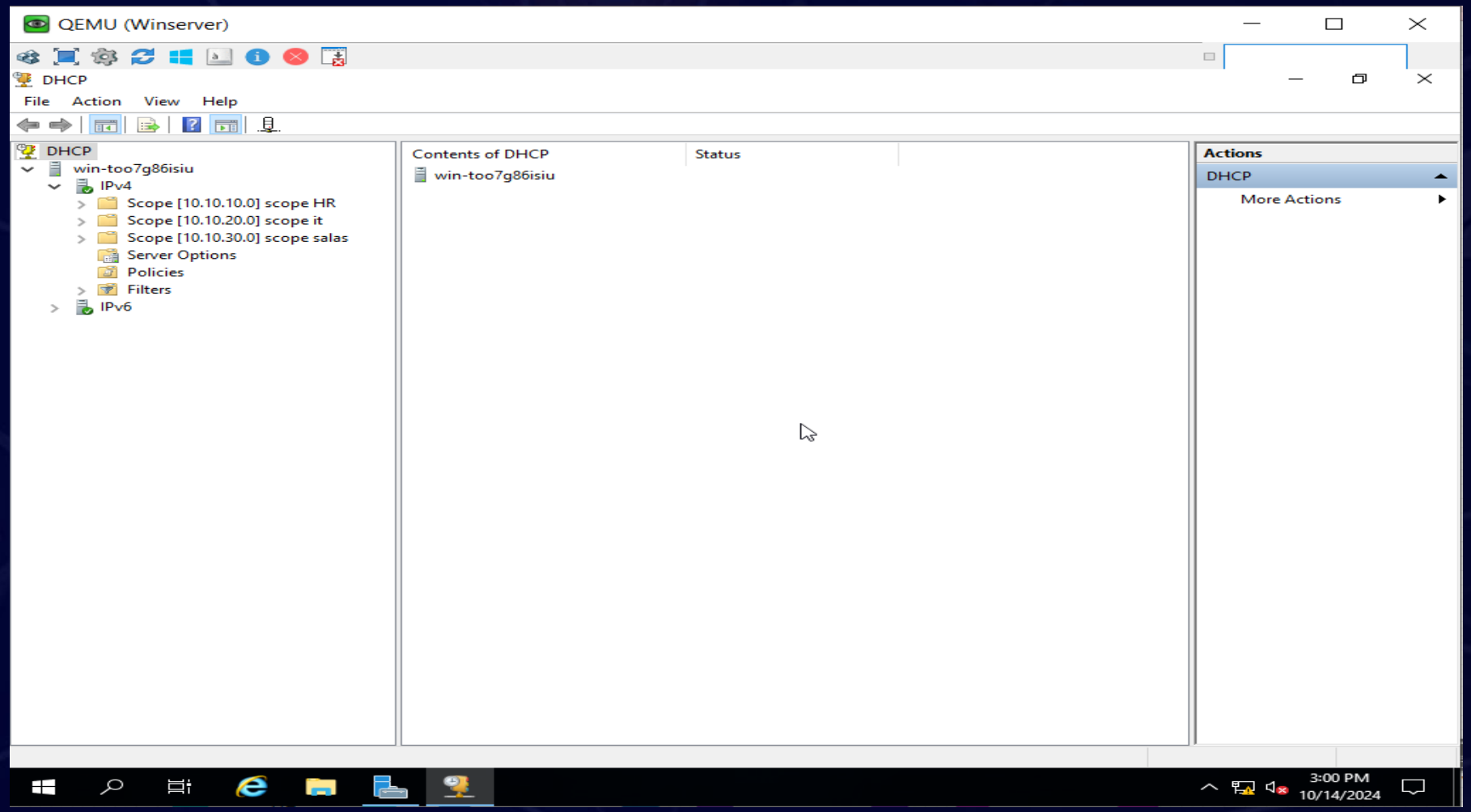
configuration

All access switch

```
en
Conf t
Int  range  e0/2-3
Switchport  trunk  encapsulation  dot1Q
Switchport  mode  trunk
Switchport  nonegotiation
Exit
Vtp  domin  cisco.com
Vtp  password  123
Vtp  version 3
Vtp  mode  client
Do  show  vlan
Spanning-tree  mode  rapid-pvst
Spanning-tree  vlan1,10,20,30,40
Ip dhcp  snooping  vlan 1,10,20,30,40
```

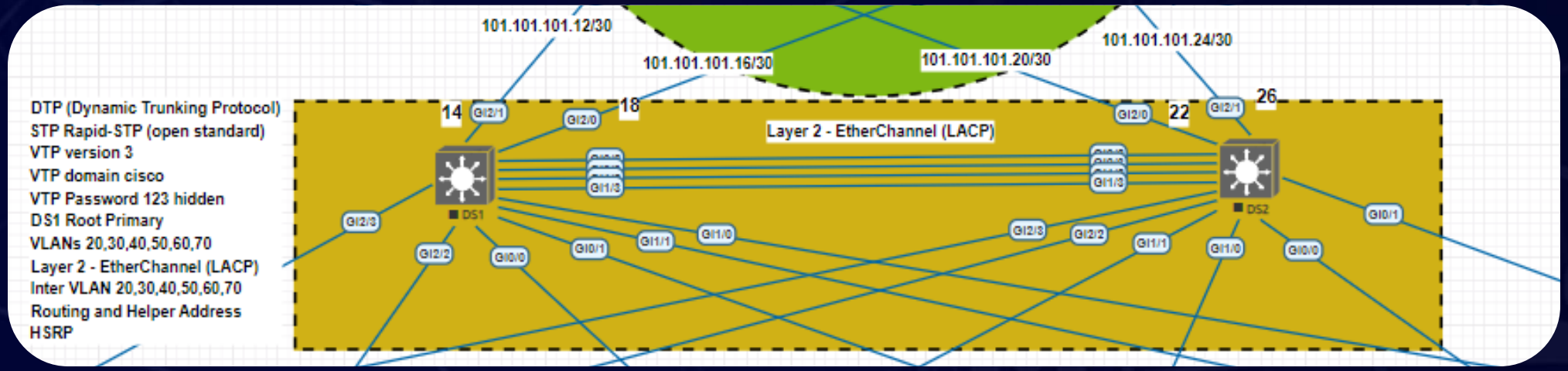
```
Int e0/0-1
Switchport  mode  access
Switchport  access  vlan 10
Spanning-tree  portfast
Spanning-tree  Bpdugard  enable
Switchport  portsecurity
Switchport  portsecurity max 1
Switchport  portsecurity  mac-address  stacky
Switchport  portsecurity  violation  shutdown
Ip dhcp  snooping l  imit-rate 4
Int  range  e0/2-3
Ip  dhcp  snooping trust
Exit
Errdisable  recovery  interval  30
Errdisable  recovery  cuase  portsecurity
```

- configuration
  - Windows server (DHCP)



3 Distribution Layer

➢ Distribution Layer



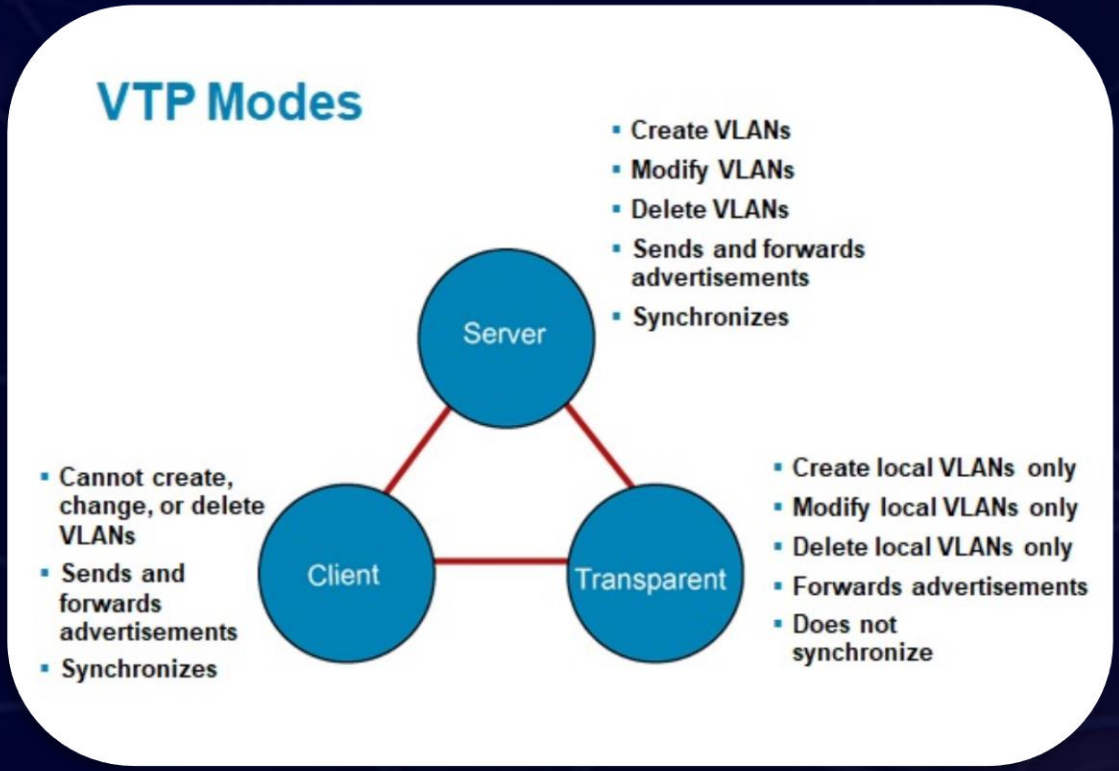
- The distribution layer is the boundary between the Layer 2 and the Layer 3 routed network.
- Layer 2 ether-channel.
- Routing services between LANs and VLANs and between routing domains.
- Redundancy.

➢ Distribution Layer

➢ VTP (VLAN Trunnking Protocol):

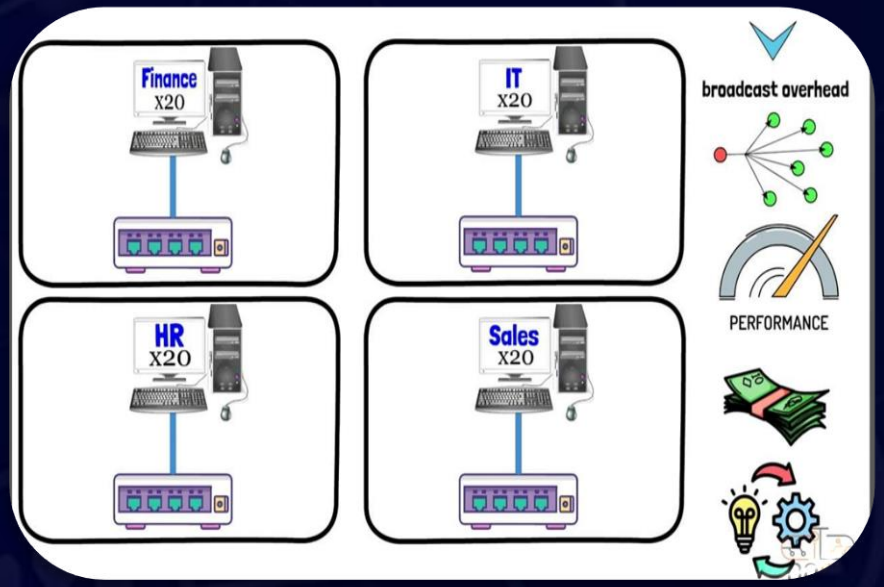
What’s VTP ?

What’s VTP V3?

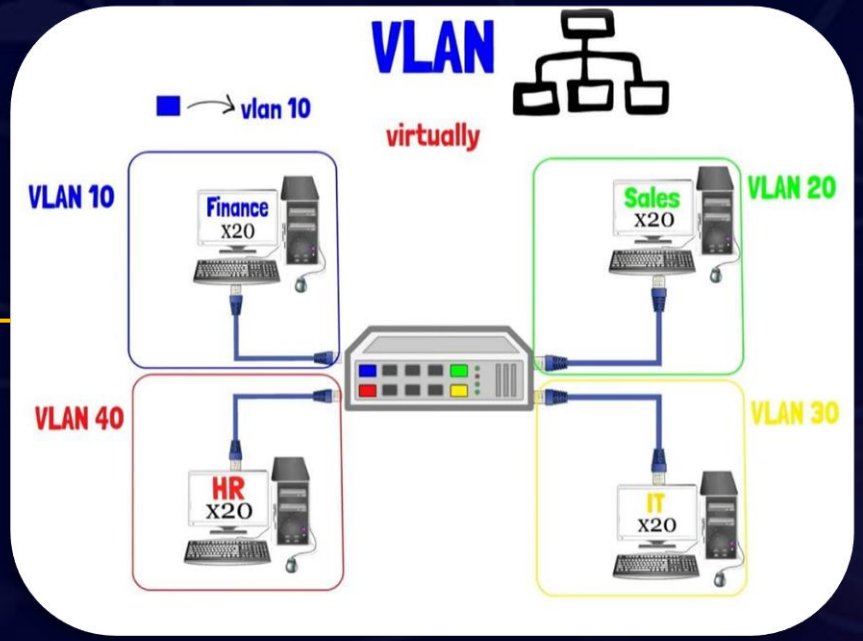


➢ VLANs (Virtual Local Area Network):

What's VLAN?

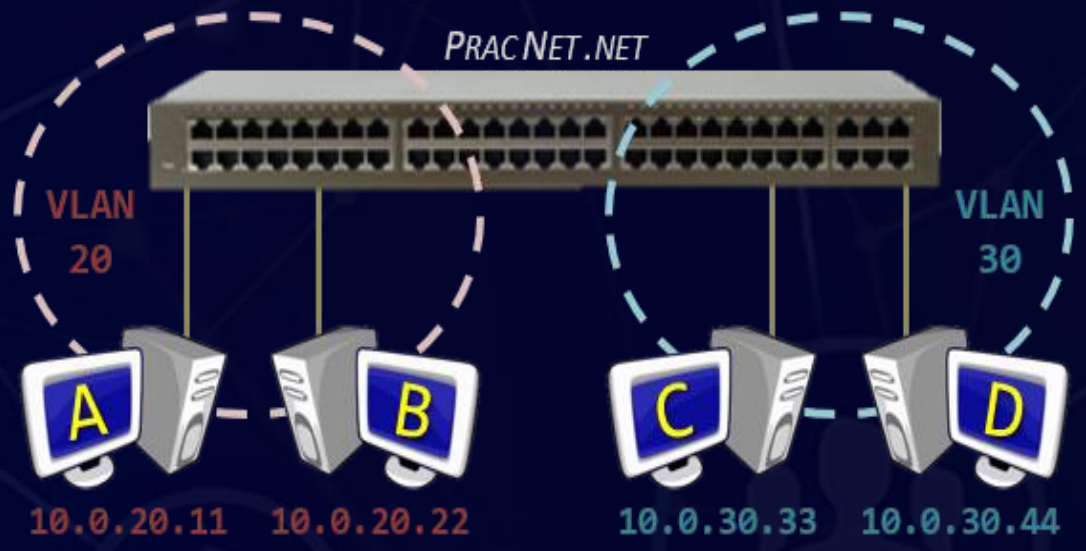


- **Advantages of a VLAN:**
  - **Separate broadcast domain.**
  - **Decrease broadcast domain.**
  - **Enhance network performance.**
  - **Scalable.**
  - **More security.**



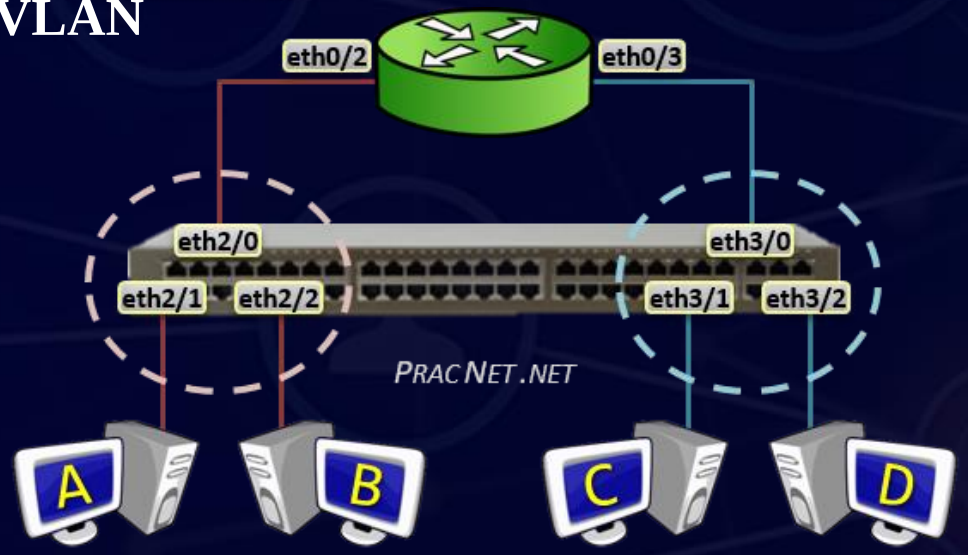
➢Routing Between VLANs

➢ **Why do we need Routing Between VLANs?**



➢ **There are three options available to enable routing between the VLANs:**

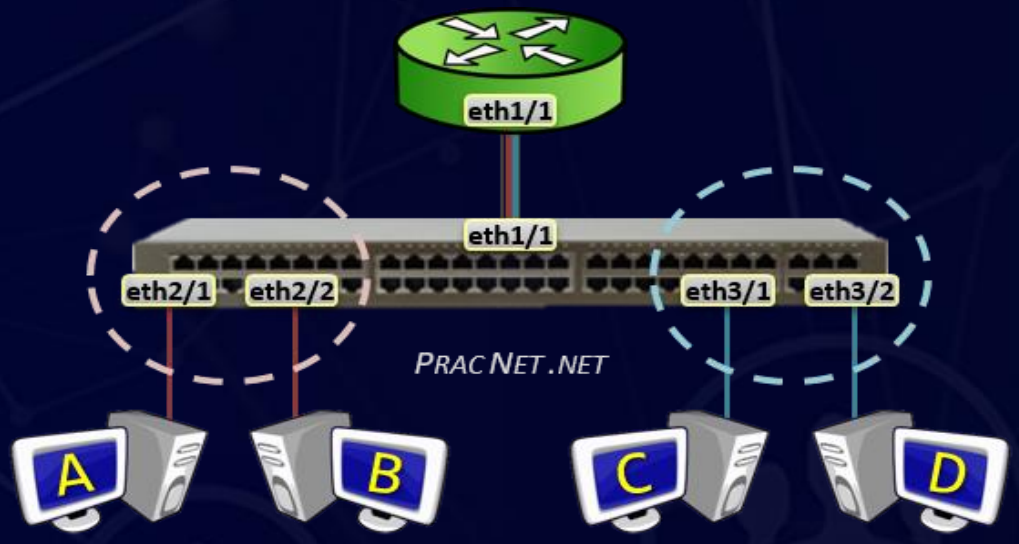
- ✓ Router with a Separate Physical Interface in each VLAN
- ✓ Router with a Sub-Interface in each VLAN
- ✓ Using a Layer 3 Switch (Best method)



➢ **Router with a Separate Physical Interface in each VLAN (Traditional Method)**

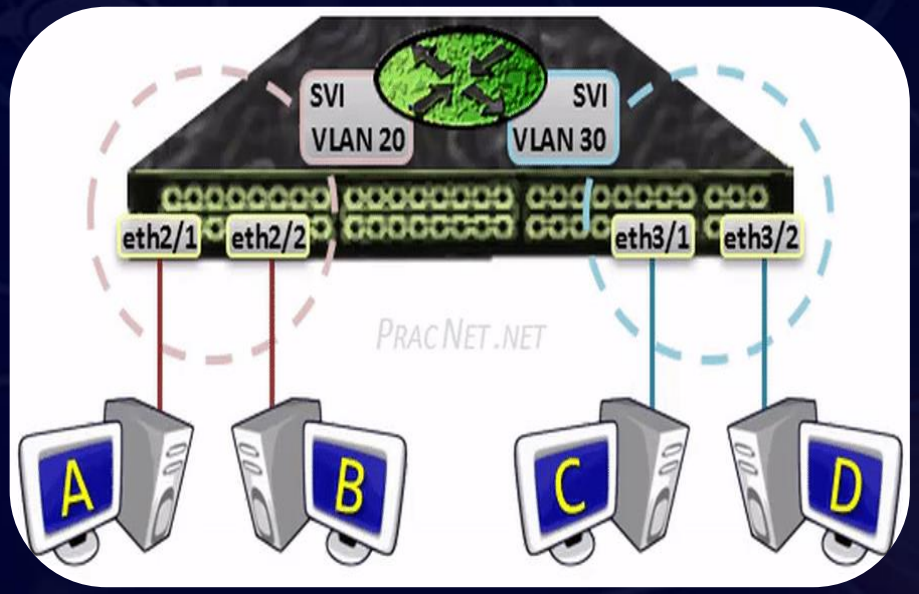
➢ Router with a Sub-Interface in each VLAN (Router on a Stick)

- ➢ A Sub-Interface allows a single Physical interface to be split up into multiple virtual sub-interfaces, each of which terminate their own VLAN.



➢ Layer 3 Switch (Best method)

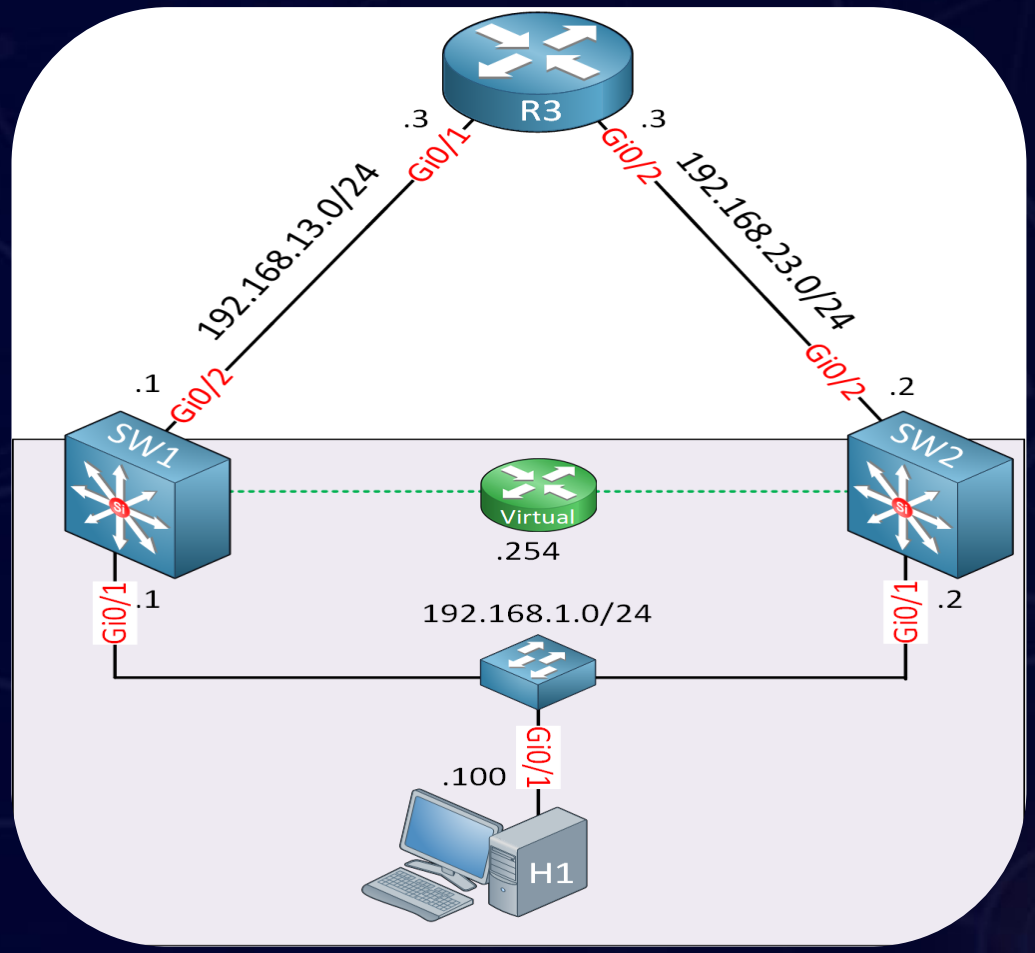
- You have the option of configuring an IP address within what is known as an SVI (Switched Virtual Interface)
- The configuration for an SVI involves two parts. First, enabling IP Routing; and Second, applying an IP address to the VLAN.
- This IP will be the default gateway for the VLAN.



➢ VRRP

What's VRRP?

- ➢ Active
- ➢ Standby
- ➢ Virtual gateway



configuration

Distribution swihch

```
en
conf t
hostname core-sw2
username cisco password cisco
banner motd & no unathorised access &
enable password cisco
service password-en
no ip domain-lookup
line console 0
login local
exec-timeout 00
logging syn
exit
```

```
ip domain-name cisco.com
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
line vty 0 15
transport input ssh
Exit
Access-list  1  permit  192.168.30.0    0.0.0.255
Access-list  1  deny  any
Line  vty  0  15
Access-class  1  in
Exit
```

configuration

Distribution swihch

```
en
conf t
vtp domain cisco.com
vtp password 123
vtp version 3

vlan 10
name HR
vlan 20
name it
vlan 30
name salas
vlan 40
name server
Exit
spanning-tree mode rapid-pvst
spanning-tree vlan 1,10,20,30,40 priority 24576

interface GigabitEthernet0/0
 no switchport
 ip address 10.10.50.2 255.255.255.0
 negotiation auto
 vrrp 50 ip 10.10.50.4
 vrrp 50 priority 150
 vrrp 50 authentication text cisco
 vrrp 50 track 1 decrement 60

interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 negotiation auto
```

➢ configuration

➢ Distribution swihch

```
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 negotiation auto
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 negotiation auto
!
interface GigabitEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 negotiation auto
```

```
interface GigabitEthernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 negotiation auto
!
interface GigabitEthernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 negotiation auto
!
interface GigabitEthernet1/2
 no switchport
 ip address 10.10.60.1 255.255.255.0
 negotiation auto
!
```

➢ configuration

➢ Distribution swihch

```
interface Vlan10
 ip address 10.10.10.2 255.255.255.0
 ip helper-address 10.10.40.4
 vrrp 10 ip 10.10.10.1
 vrrp 10 priority 150
 vrrp 10 authentication text cisco
 vrrp 10 track 1 decrement 60
!
interface Vlan20
 ip address 10.10.20.2 255.255.255.0
 ip helper-address 10.10.40.4
 vrrp 20 ip 10.10.20.1
 vrrp 20 priority 150
 vrrp 20 authentication text cisco
 vrrp 20 track 1 decrement 60
!
```

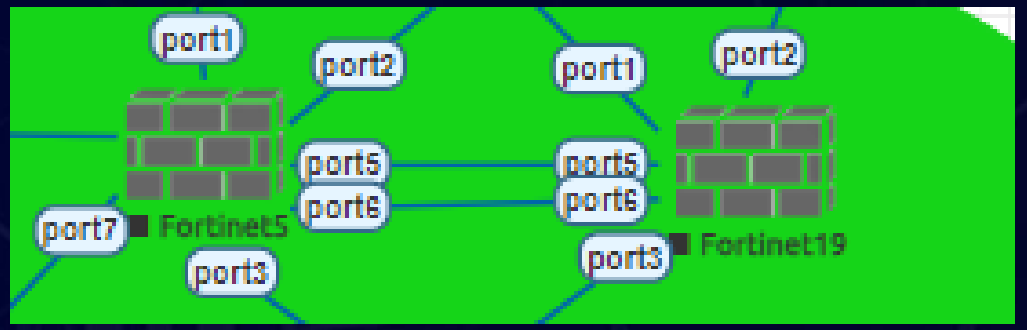
```
interface Vlan30
 ip address 10.10.30.2 255.255.255.0
 ip helper-address 10.10.40.4
 vrrp 30 ip 10.10.30.1
 vrrp 30 priority 150
 vrrp 30 authentication text cisco
 vrrp 30 track 1 decrement 60
!
interface Vlan40
 ip address 10.10.40.2 255.255.255.0
 vrrp 40 ip 10.10.40.1
 vrrp 40 priority 150
 vrrp 40 authentication text cisco
 vrrp 40 track 1 decrement 60
!
ip route  0.0.0.0  0.0.0.0  10.10.50.1
```

4 Firewall

➢ Firewall

- A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules

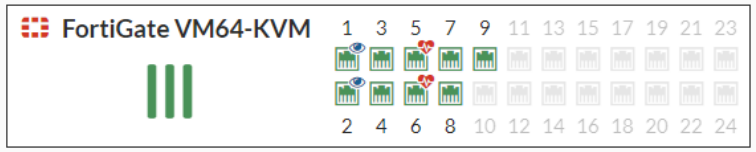
- Its primary function is to establish a barrier between trusted internal networks and untrusted external networks, such as the internet, to prevent unauthorized access and potential threats.



➢ Firewall

➢ High Availability (HA)

- High Availability (HA) in FortiGate firewalls provides redundancy by using multiple devices. If one fails, another takes over to ensure continuous service without downtime.



FGT-master (Primary)

Refresh | Edit | Remove device from HA cluster

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
Synchronized	150	FGT-master	FGVMEVBVMKSKUG31	Primary	23m 41s	0	65.00 kbps

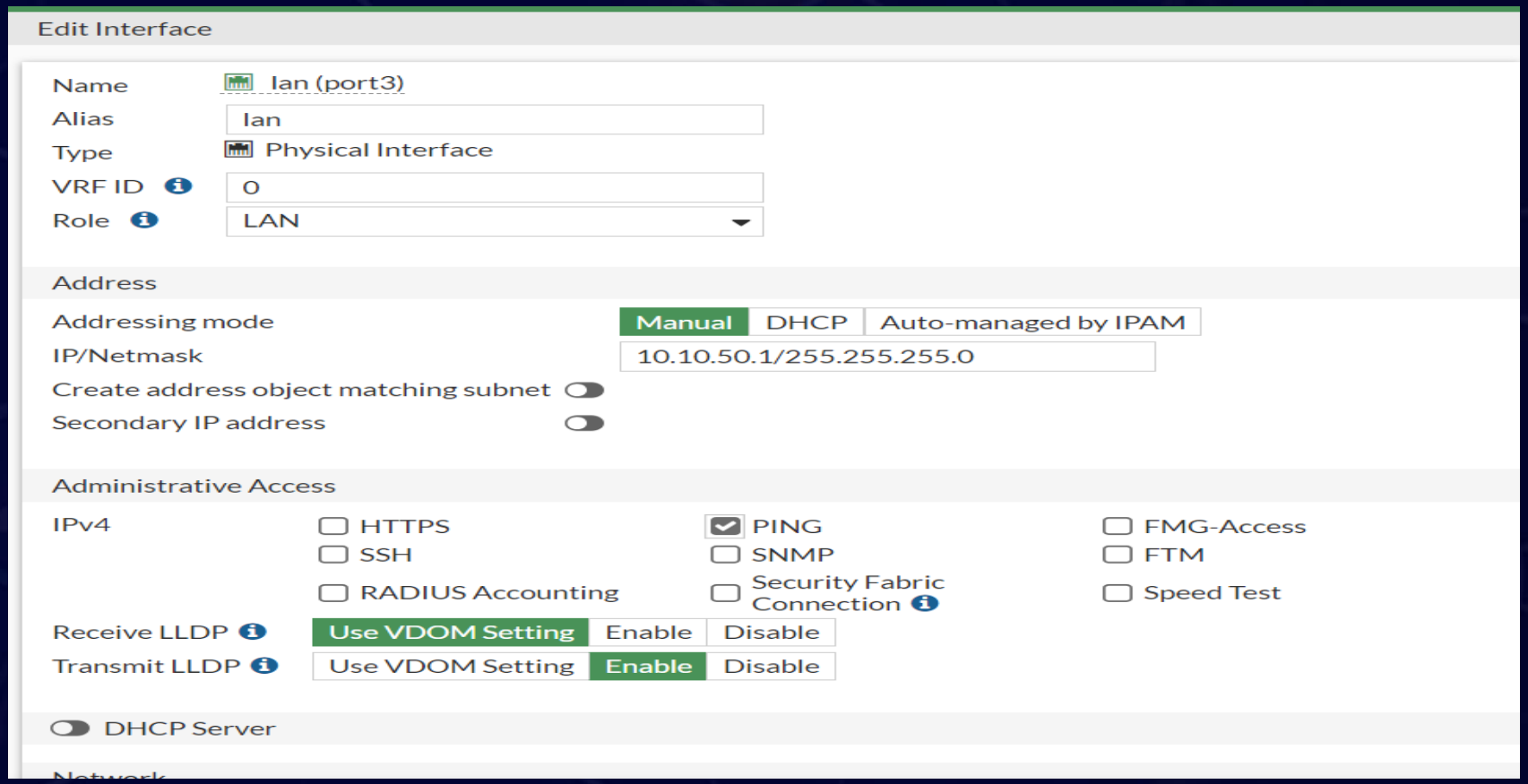
➢ Firewall

➢ Interface (WAN PORT)

	vpn (port4)	Physical Interface		192.168.201.1/255.255.255.0	PING
	WAN Orange (port1)	Physical Interface		200.20.20.1/255.255.255.0	PING HTTPS SSH HTTP FMG-Access
	WAN We (port2)	Physical Interface		100.10.10.2/255.255.255.0	PING HTTPS SSH FMG-Access

➢ Firewall

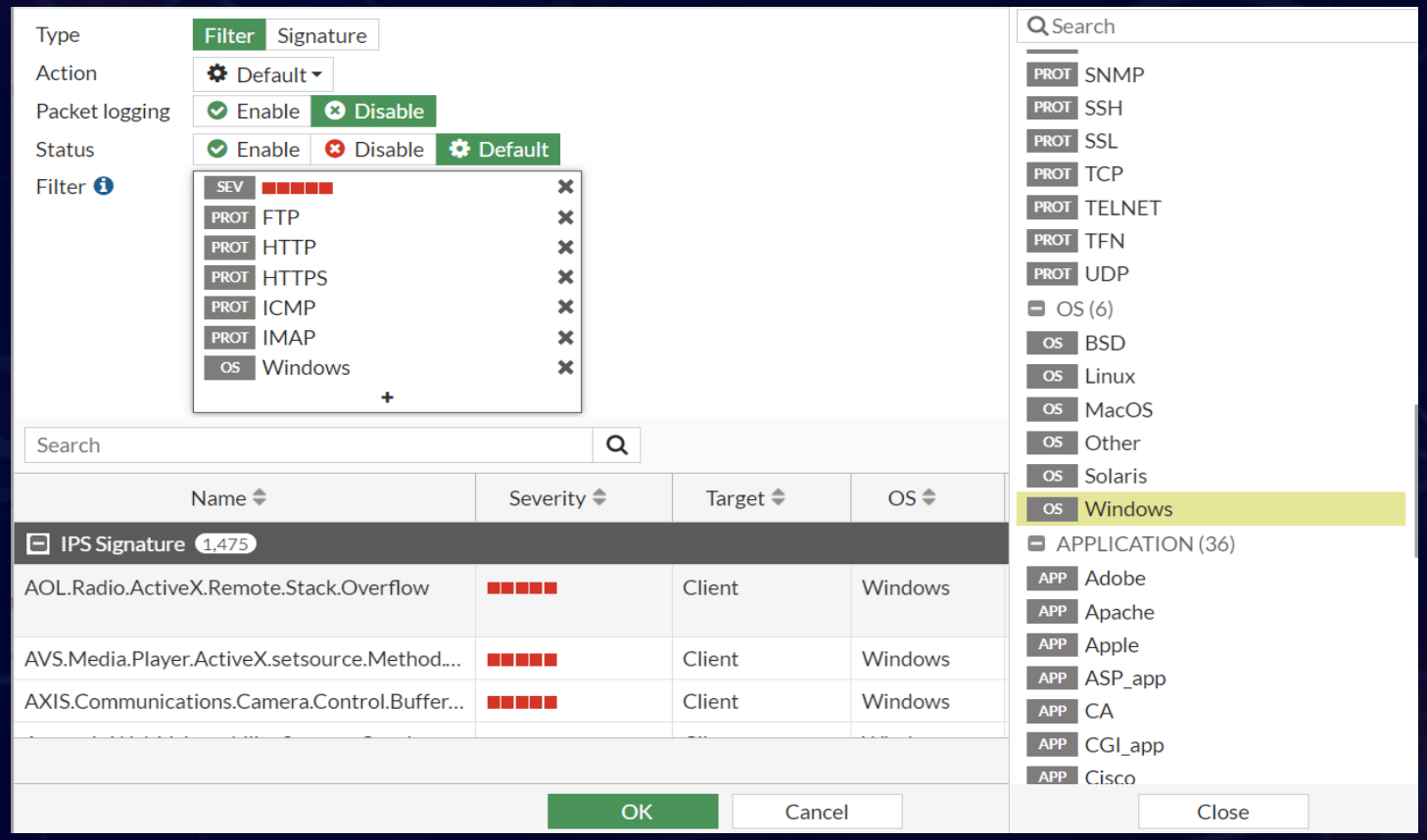
➢ Interface (LAN PORT)



➢ Firewall

➢ Security profile (IPS)

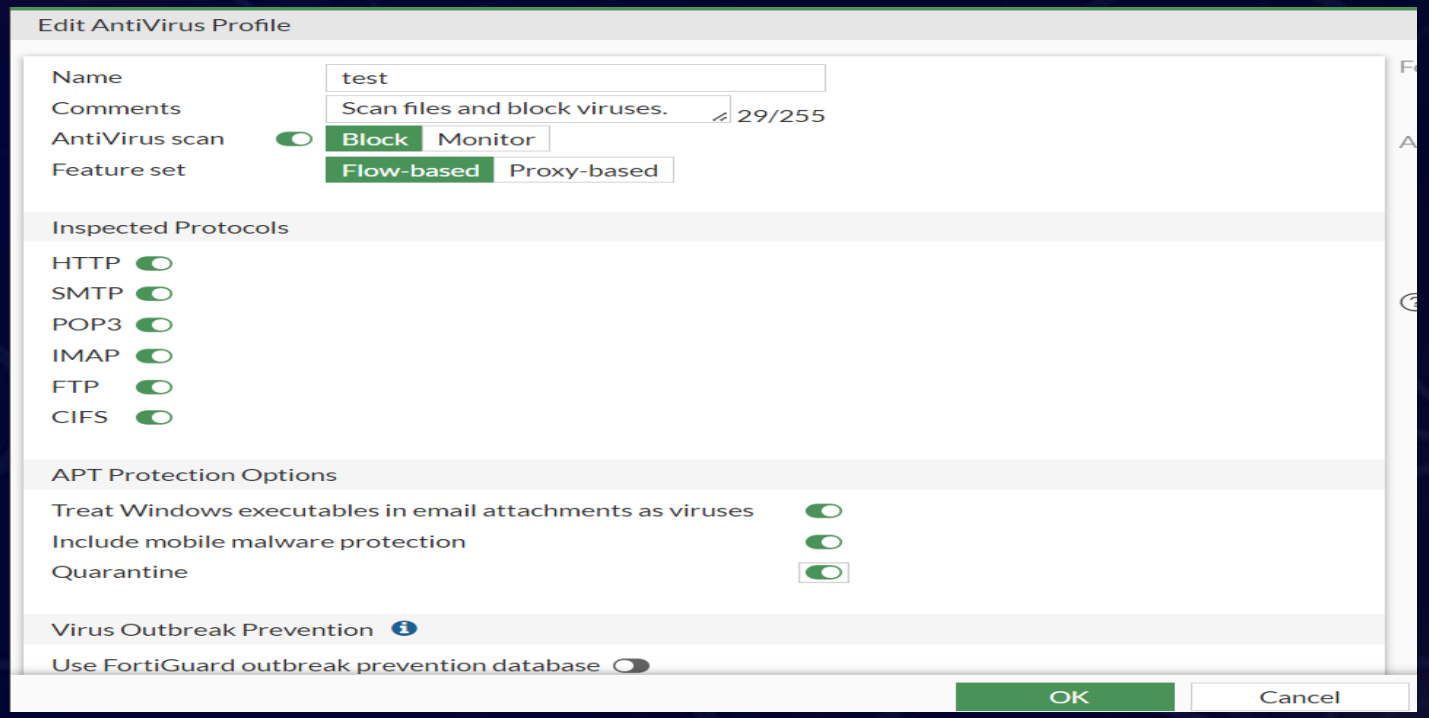
- The IPS (Intrusion Prevention System) in FortiGate inspects network traffic for malicious activity and potential threats, such as intrusion attempts or vulnerability exploits. It automatically blocks or alerts on detected threats to protect the network in real time.



➢ Firewall

➢ Security profile (antivirus)

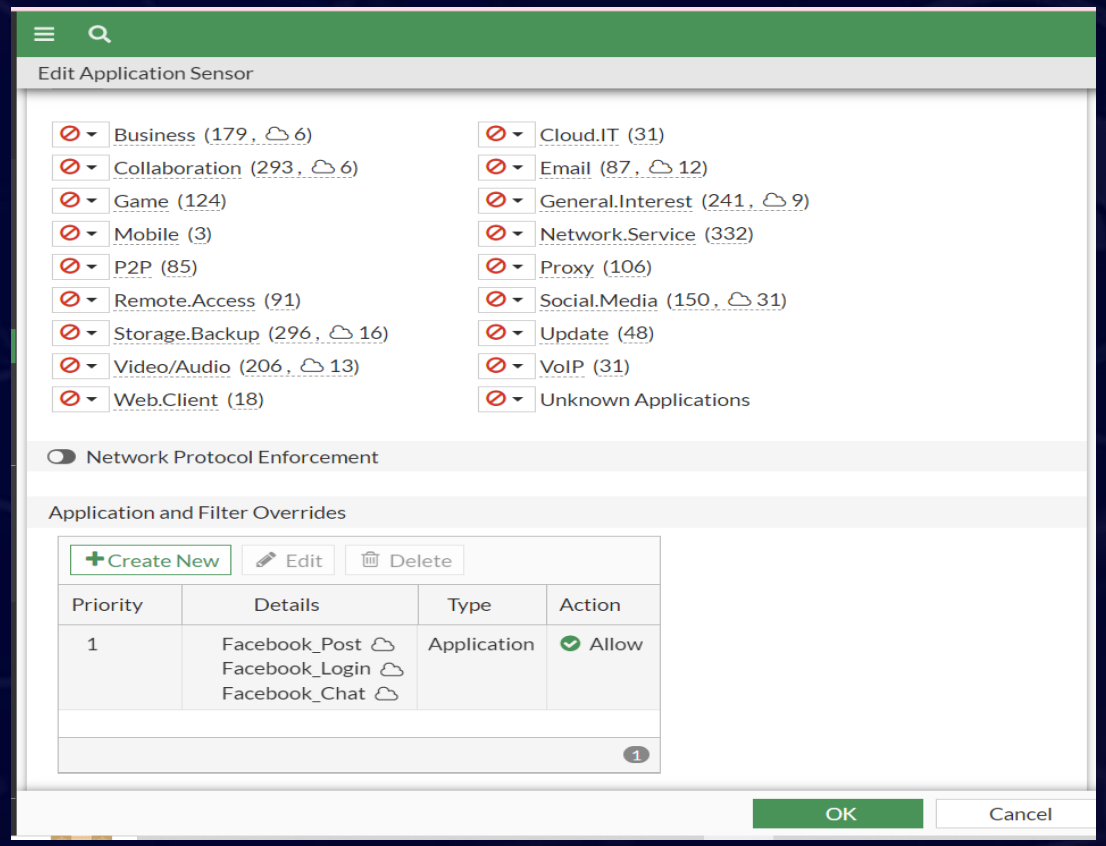
- The antivirus feature in FortiGate scans network traffic and files for viruses, malware, and other malicious content. It prevents infections by detecting and blocking harmful files before they can reach devices on the network.



➢ Firewall

➢ Security profile (web filter)

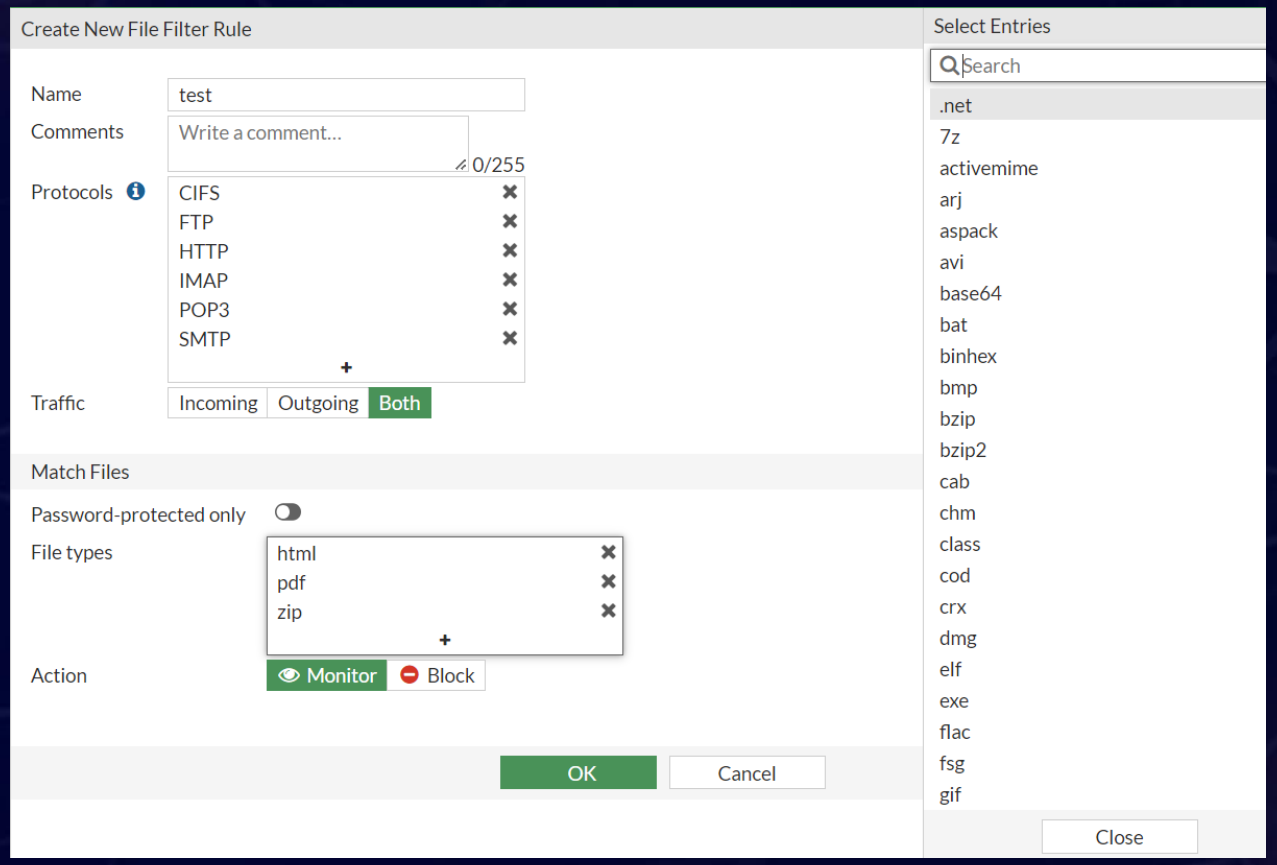
- The web filtering feature in FortiGate controls access to websites by categorizing and blocking harmful or inappropriate content. It helps enforce security policies and protect users from malicious sites, phishing, and other online threats.



➢ Firewall

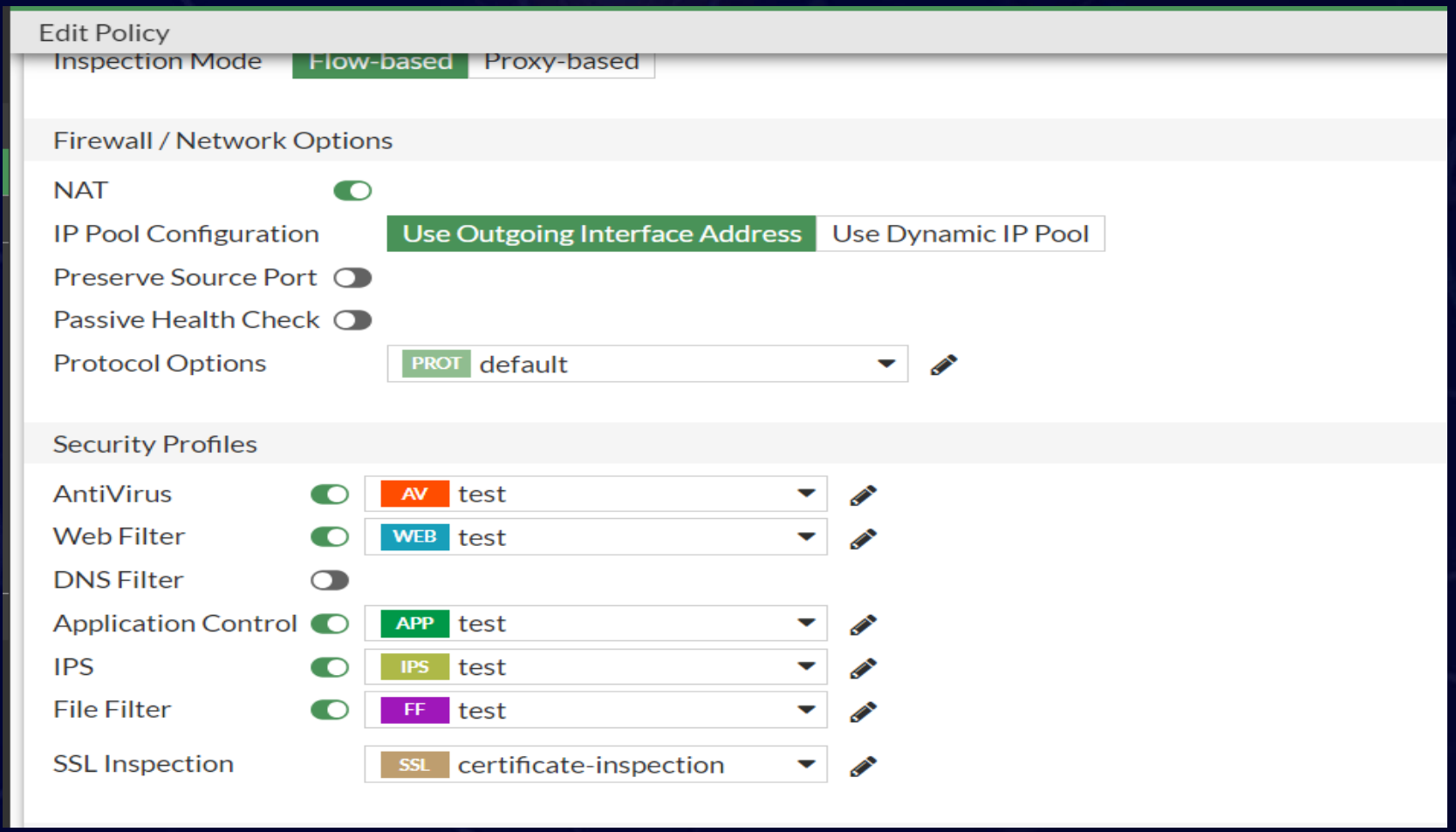
➢ Security profile (file filter)

- The file filter feature in FortiGate blocks or restricts access to specific file types within network traffic. It helps prevent the transfer of unauthorized or malicious files, enhancing data security and compliance.



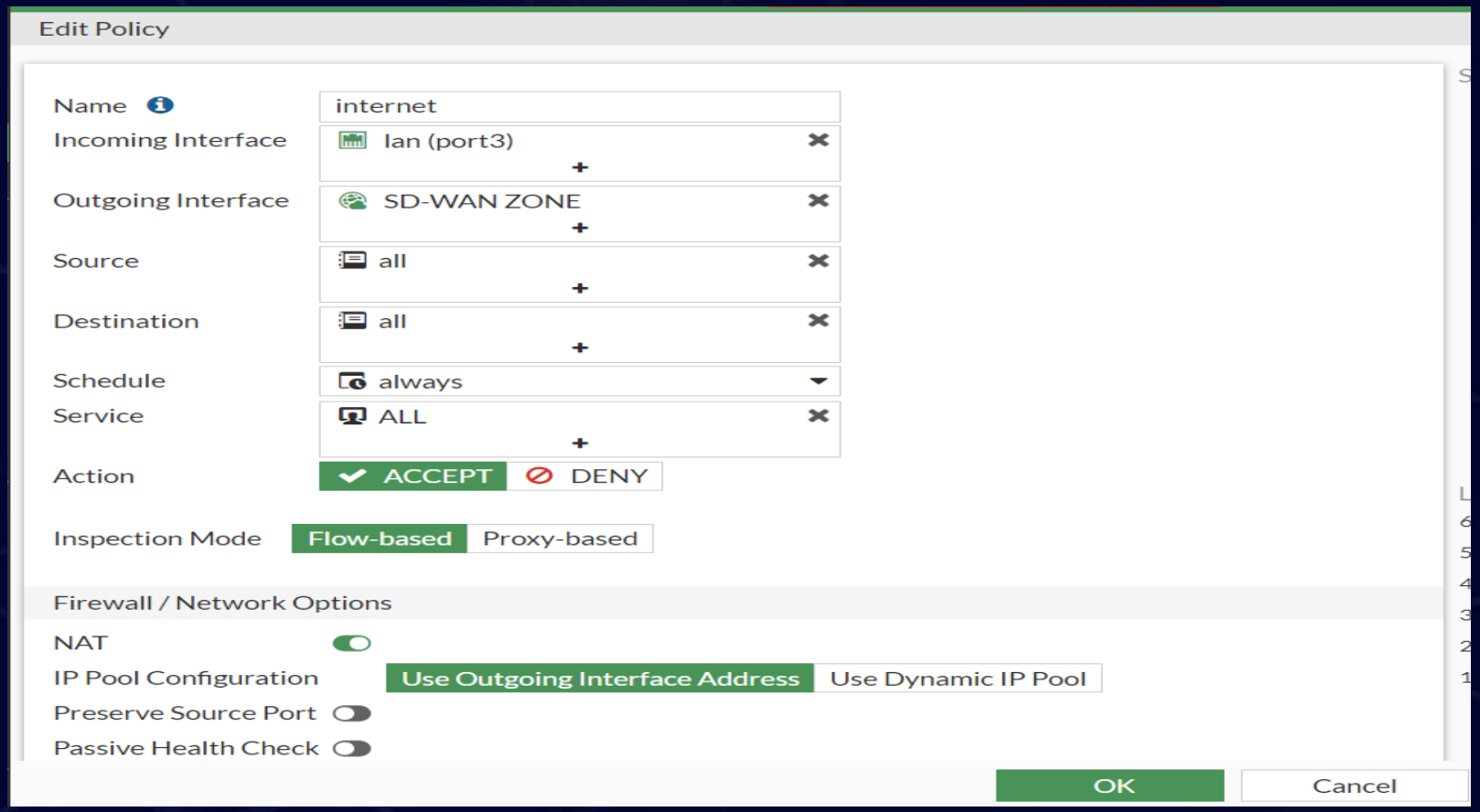
➢ Firewall

➢ Security profile (In policy)



➢ Firewall

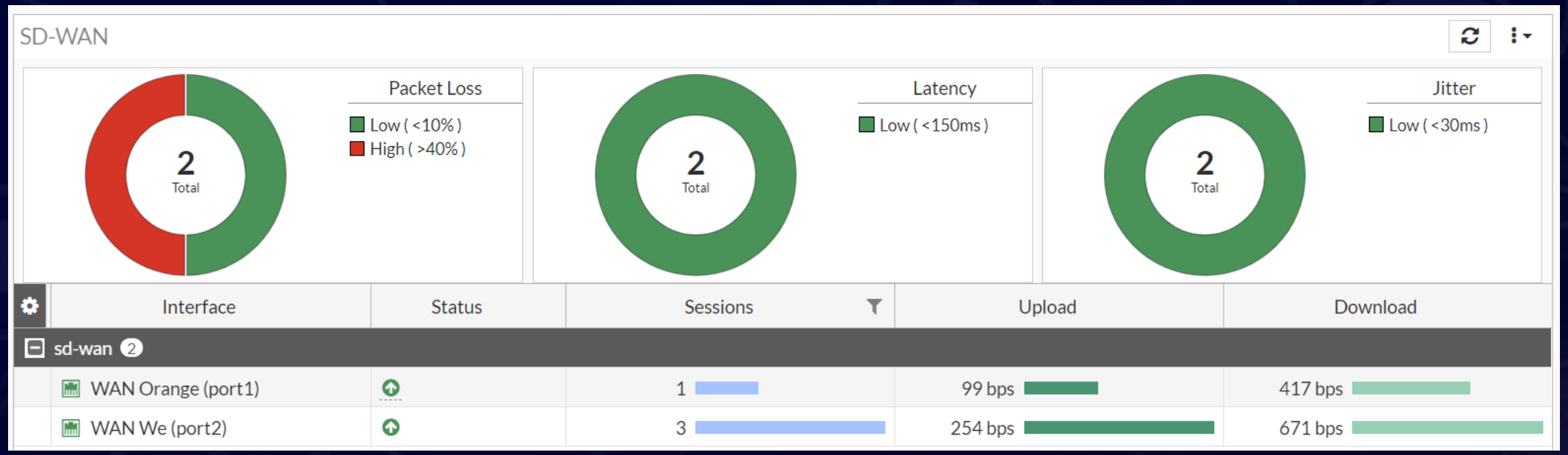
➢ Internet policy



5 SD-WAN

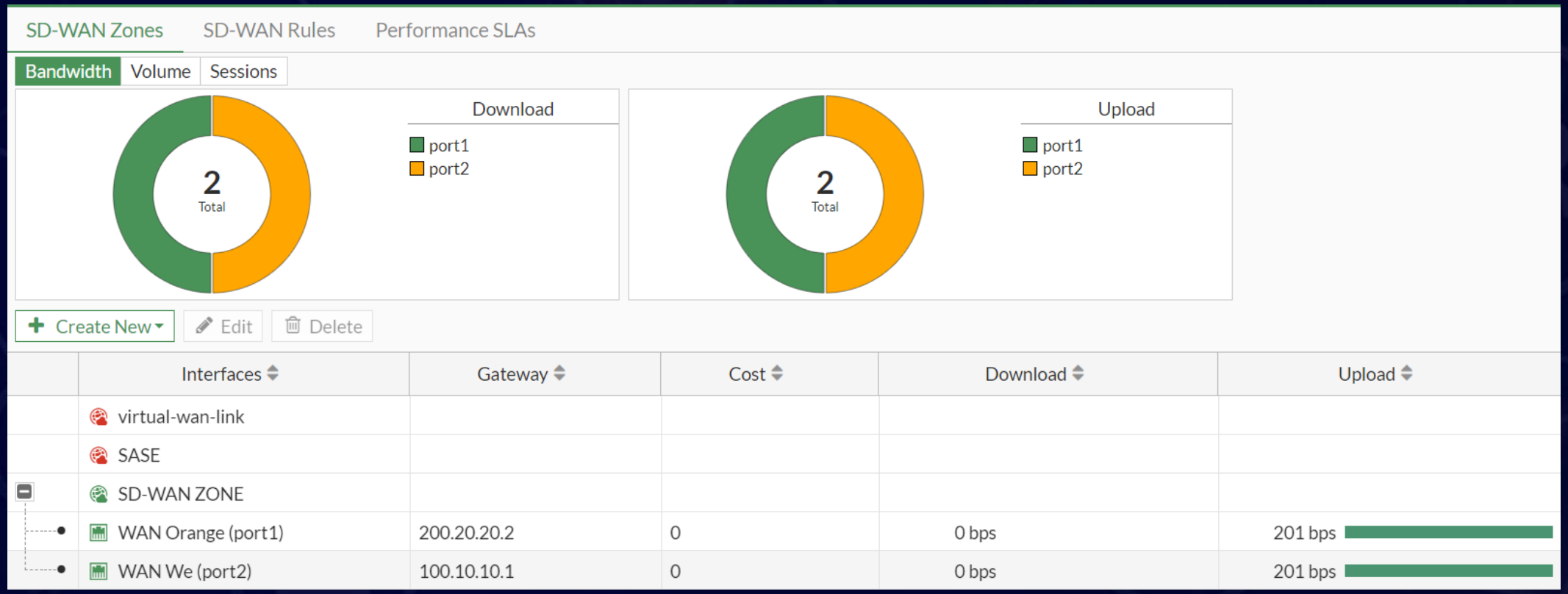
➢ SD-WAN

- The SD-WAN feature in FortiGate optimizes and manages multiple WAN connections, improving performance and reliability. It intelligently routes traffic based on application needs, ensuring secure and efficient connectivity across different network paths.



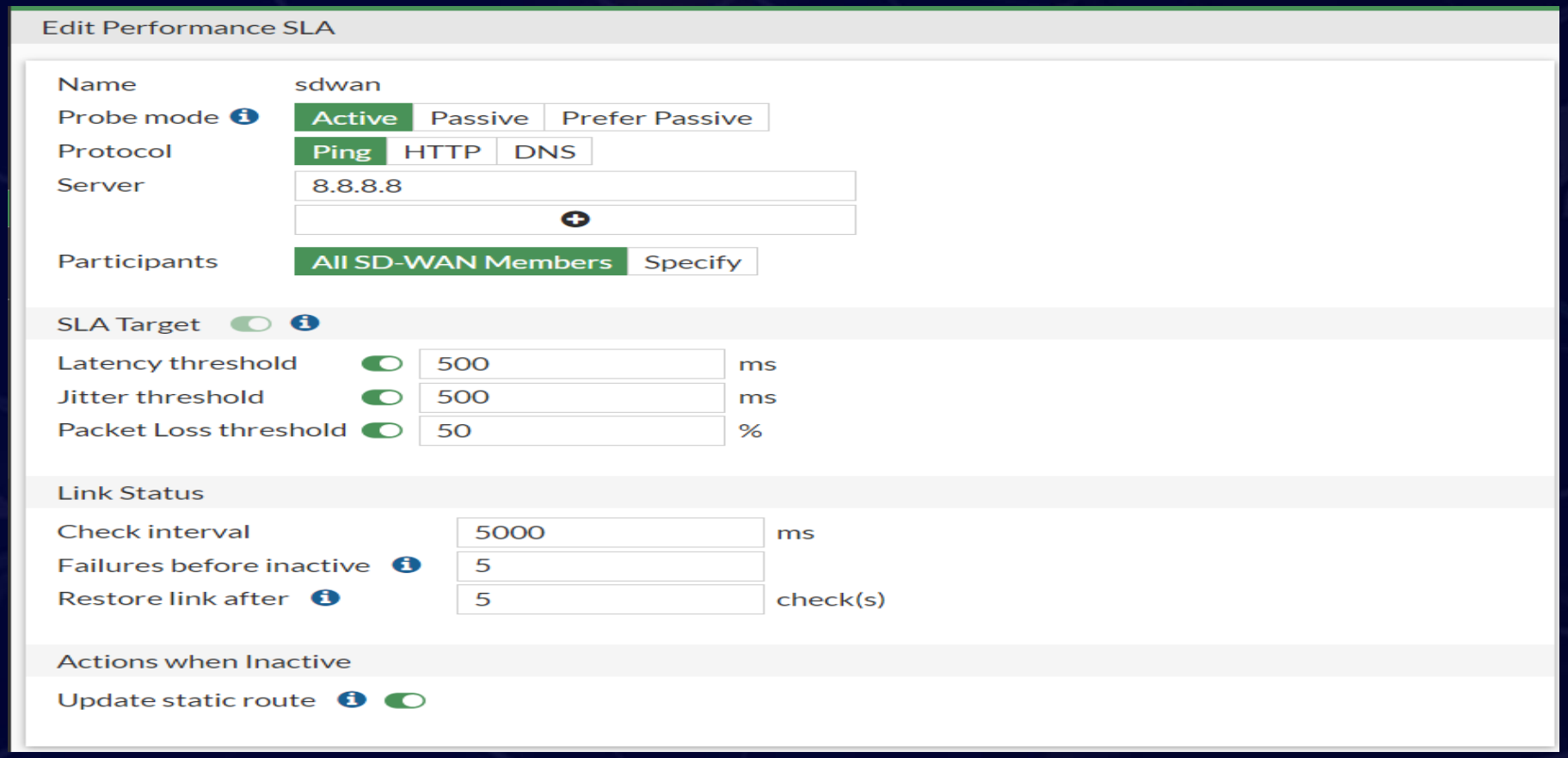
➢ SD-WAN

➢ Sd-wan zone



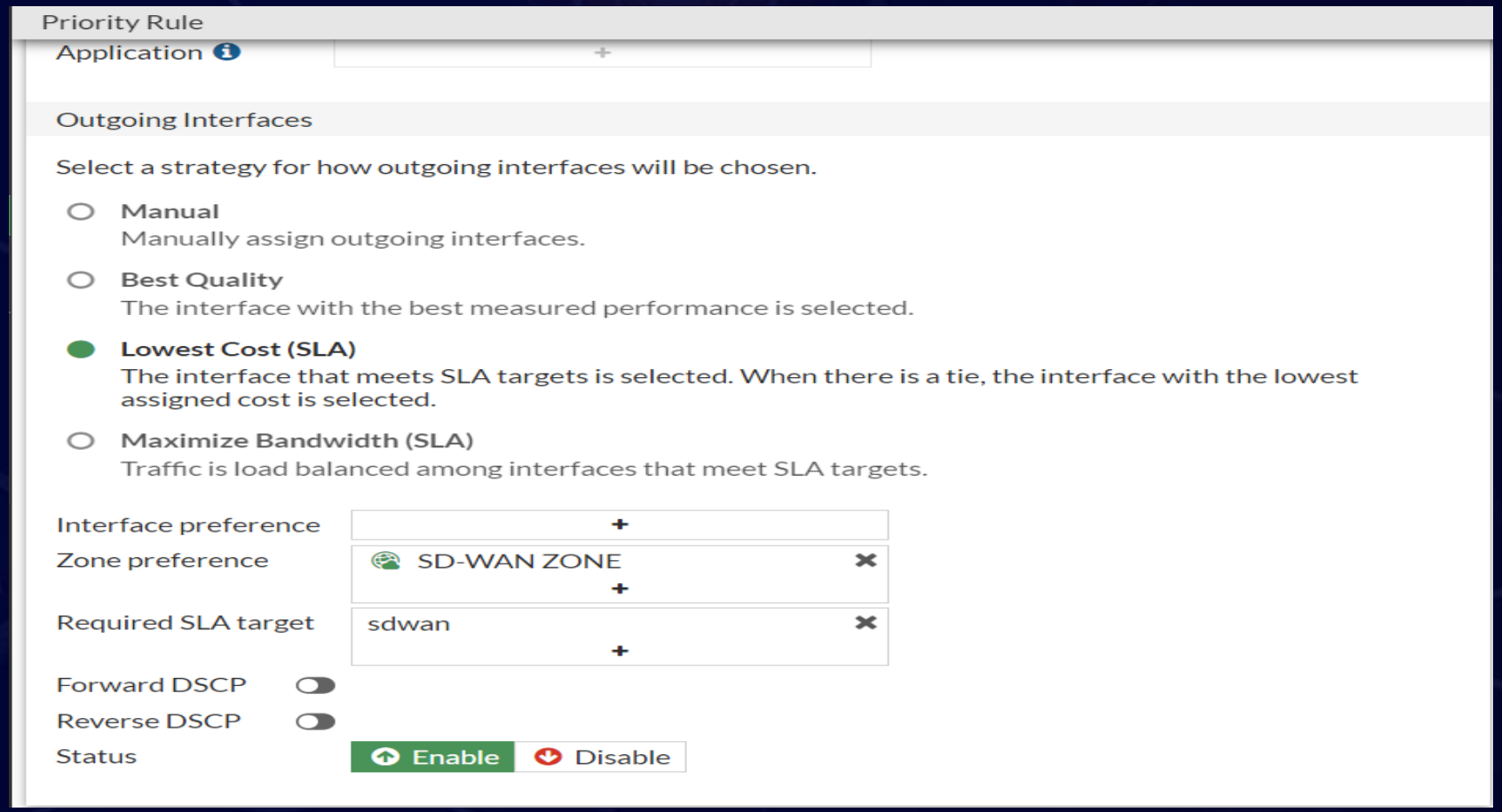
➢ SD-WAN

➢ Sd-wan LSA



➢ SD-WAN

➢ Sd-wan Role

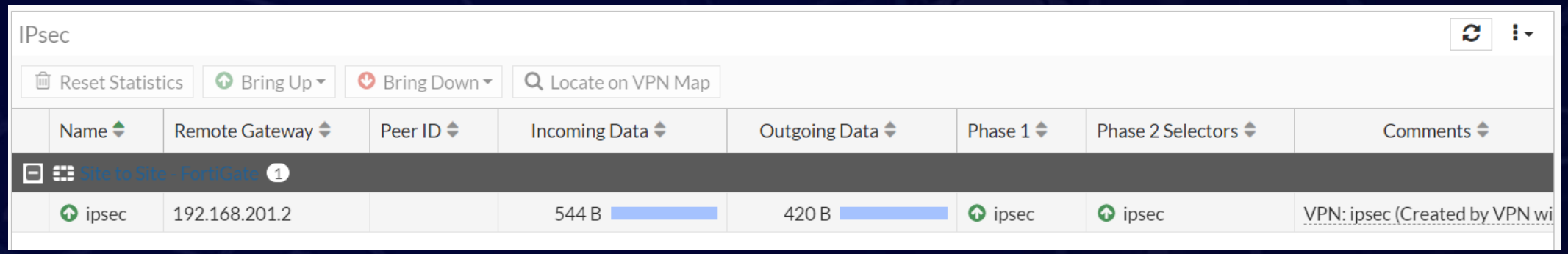


6 VPN

➢ VPN

➢ Site to site vpn

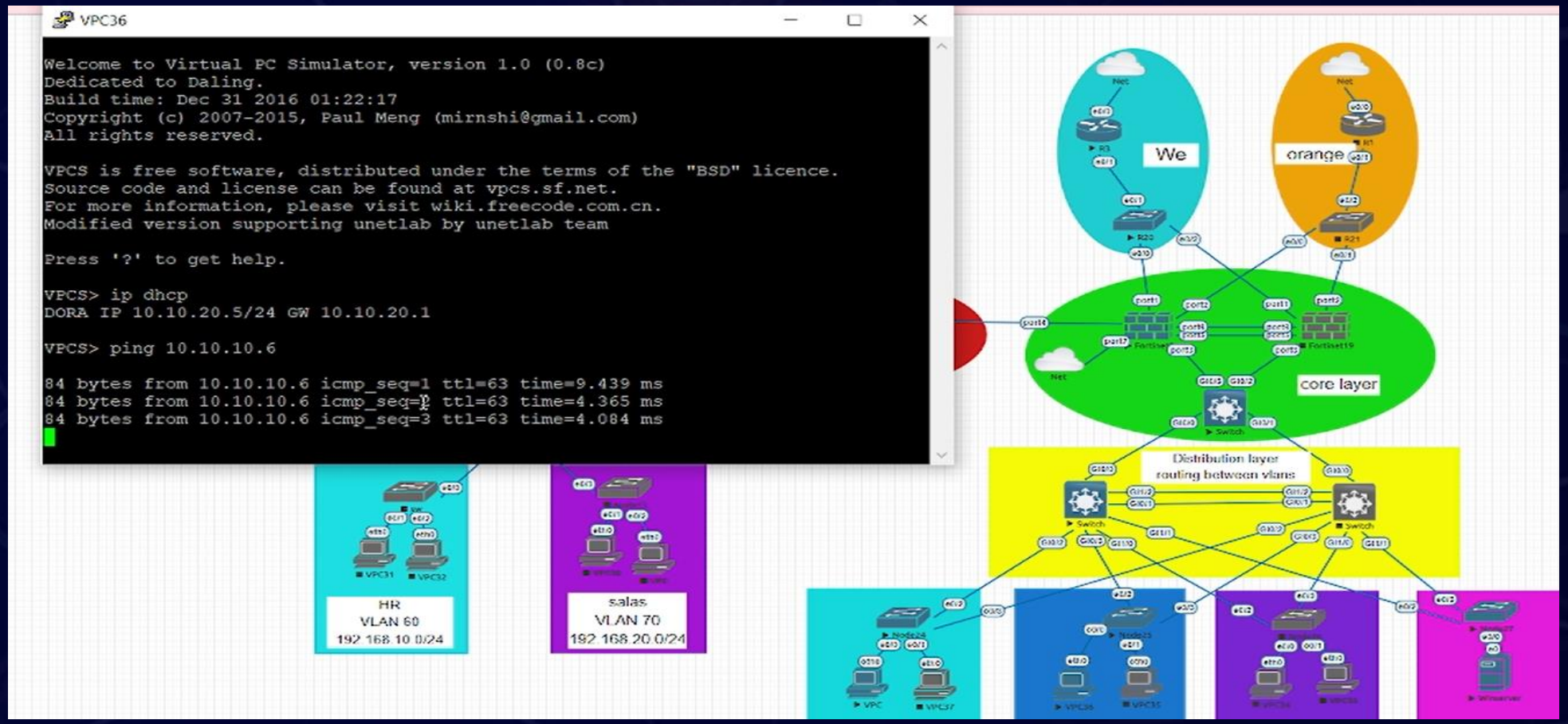
- The site-to-site VPN in FortiGate establishes secure, encrypted tunnels between different networks over the internet. It enables seamless communication between remote sites, ensuring data confidentiality and integrity while allowing centralized management and access control



7 Tests

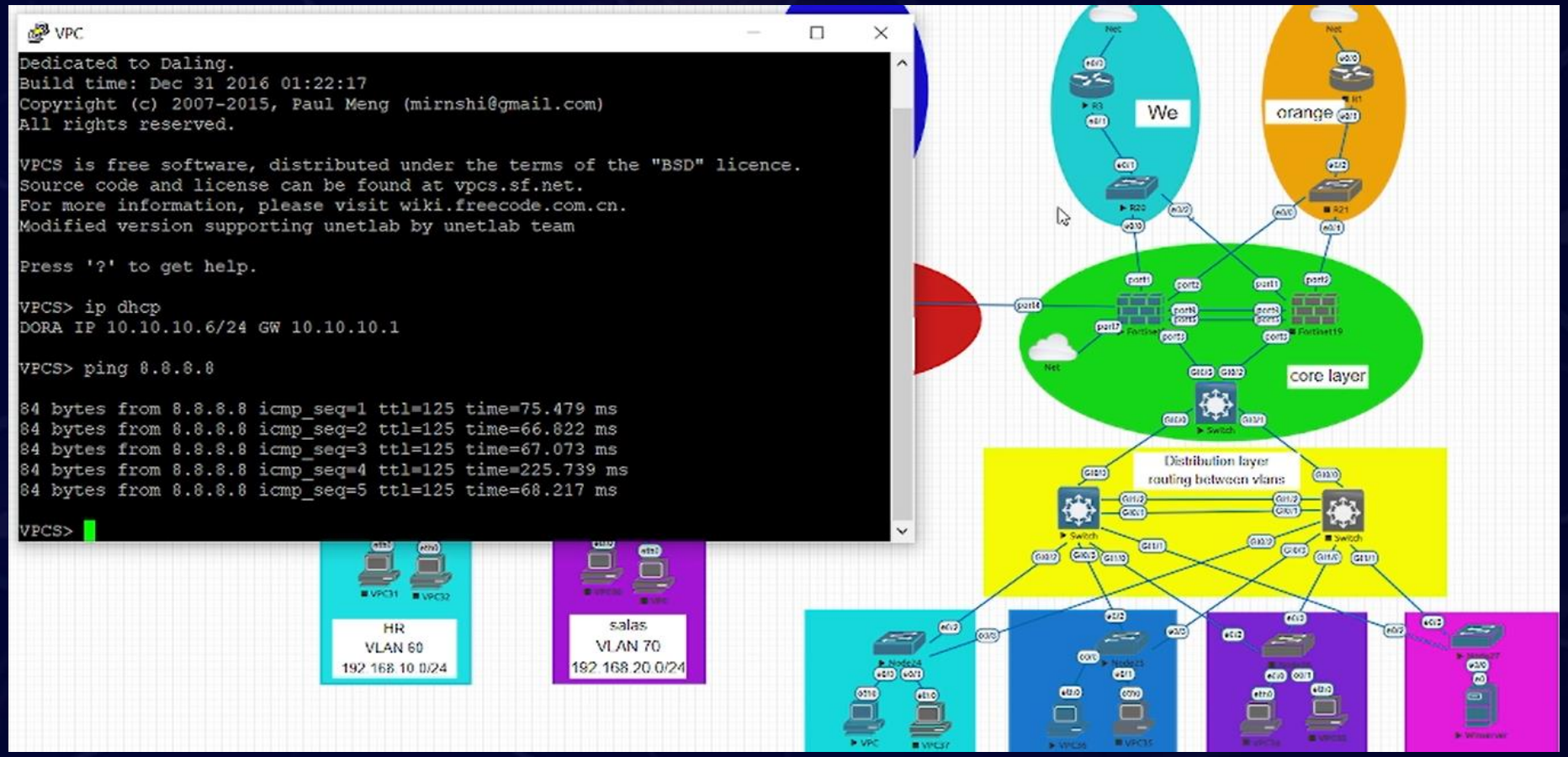
➢ Test

➢ Test routing between vlan



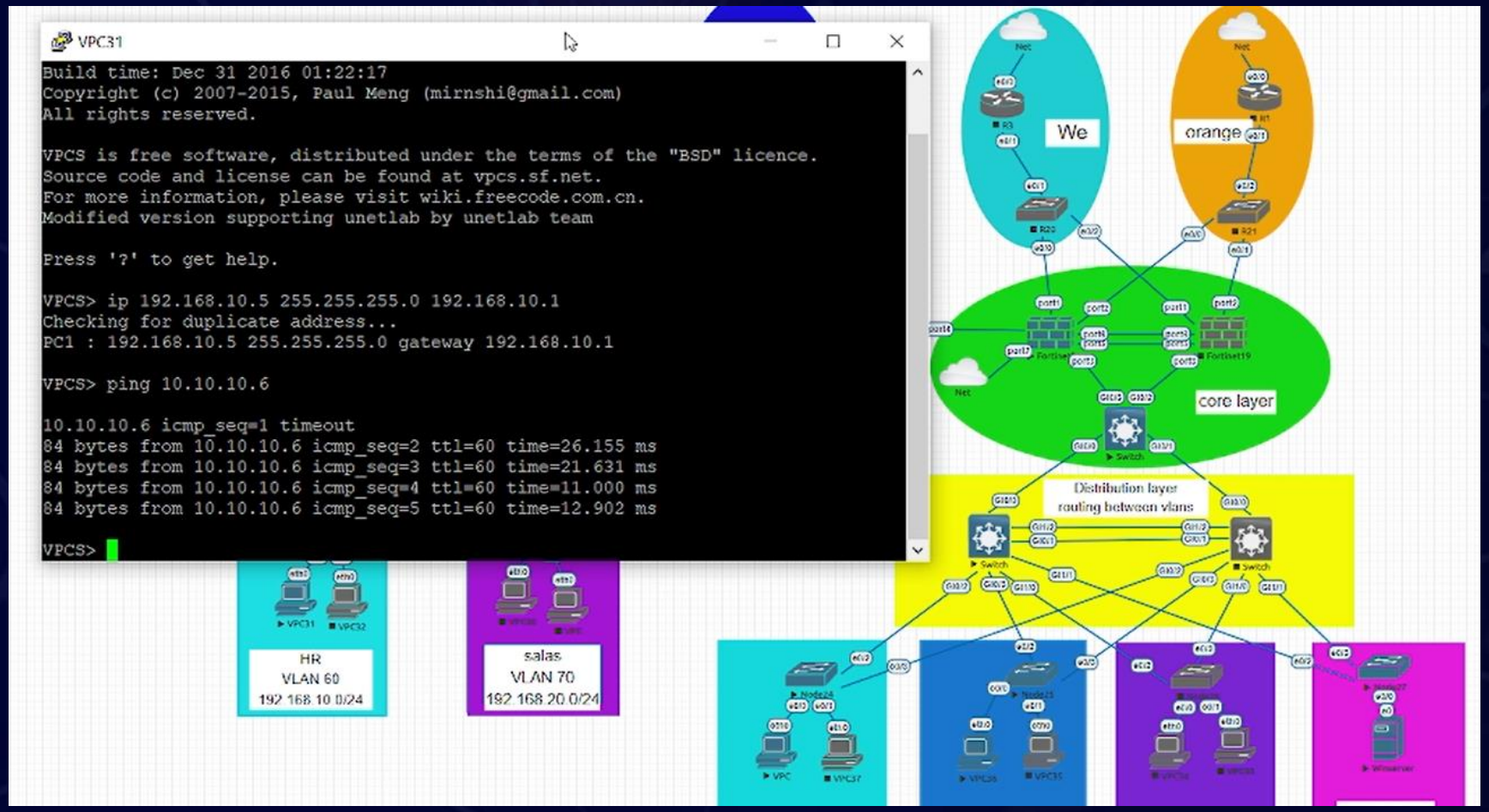
➢ Test

➢ Test internet



➢ Test

➢ Test conectivity between two sites



Thank You

For your time